MEV and the Proposer’s Monopoly on Inclusion

MEV and the Proposer’s Monopoly on Inclusion

Modern blockchains operate on a leader-based system where a rotating proposer holds the power to decide which transactions are included in each block and what order to include them in. Some proposers collude with MEV-searchers to maximize the rents that they can extract from this temporary monopoly (e.g. MEV boost). The value extracted is far from pennies, and is estimated to be worth billions of dollars a year on Ethereum.

best guess order of magnitude based on conversations with players

atomic arb on eth: ~$1b / year

stat arb on eth: ~$10b / year

long tail arb on eth: ~$1-5b / year

high confidence on atomic, 50% confidence interval on stat arb

would love to see disproving data! https://t.co/Y57my4lnQD

— Stephane (@thegostep) May 17, 2022

best guess order of magnitude based on conversations with players

atomic arb on eth: ~$1b / year

stat arb on eth: ~$10b / year

long tail arb on eth: ~$1-5b / year

high confidence on atomic, 50% confidence interval on stat arb

would love to see disproving data! https://t.co/Y57my4lnQD

— Stephane (@thegostep) May 17, 2022

best guess order of magnitude based on conversations with players

atomic arb on eth: ~$1b / year

stat arb on eth: ~$10b / year

long tail arb on eth: ~$1-5b / year

high confidence on atomic, 50% confidence interval on stat arb

would love to see disproving data! https://t.co/Y57my4lnQD

https://t.co/Y57my4lnQDMay 17, 2022

Now imagine if a chain could capture all that value and return it back to users in the process. Impermanent loss for liquidity providing wouldn’t exist! Luckily, auctions are a great mechanism for selling complex bundles of resources such as blockspace. Unluckily, on-chain auction designs have a major vulnerability. Malicious block proposers are given a monopoly on transaction inclusion

Malicious block proposers are given a monopoly on transaction inclusionThe proposer’s monopoly on inclusion is the weak link, which allows for cheap censorship. In order to improve the censorship resistance of a chain we need to destroy this monopoly by allowing multiple concurrent block proposers (MCBP). In particular, we would like to expand the set of nodes who are able to contribute transactions in each block. Multiplicity is a practical gadget that allows non-leader nodes to include additional transactions into a block.

Multiplicity: A Practical Gadget for Multiple Concurrent Proposers

:

Multiplicity: A Practical Gadget for Multiple Concurrent Proposers

Informally, In the first stage every non-byzantine validator on the committee sends a signed special bundle of transactions, to the leader. In order to construct a valid block, the leader must include at least 2/3 (stake weighted) of these bundles. Therefore the leader cannot construct a valid block that omits a transaction which was included in >1/3 (stake weighted) of the special bundles.

More formally: a proposed block is only valid if the leader includes a sufficient quorum (defined either by stake-weight or number) of validator-signed special bundles of transactions.

The gadget adds the additional steps to proof-of-stake protocols:

1. Each validator constructs a special bundle of transactions from their local view of the mempool. They sign this and send it to the leader.

2. Based on payloads received from other validators, the leader creates, signs and broadcasts a block proposal containing at least 2/3 (stake weighted) of these special bundles. .

3. When determining the validity of the leader's proposal, validators check that sufficiently many special bundles are included in the block

Each validator constructs a special bundle of transactions from their local view of the mempool. They sign this and send it to the leader.

Based on payloads received from other validators, the leader creates, signs and broadcasts a block proposal containing at least 2/3 (stake weighted) of these special bundles. .

When determining the validity of the leader's proposal, validators check that sufficiently many special bundles are included in the block

3a. If the block contains a quorum of payloads the block is sufficient and consensus proceeds normally.

3b. If the block does not contain a quorum of payloads it is considered invalid and a new round of consensus starts the same way it would if a block contained a transaction with an invalid signature.

Conditional Tipping Logic to Incentivize Inclusion

Conditional Tipping Logic to Incentivize Inclusion

Conditional tipping rules where the transaction tip is only split among the proposers who include a transaction can be used to improve censorship resistance even further. Conditional tipping logic increases the cost of censorship by making colluding equilibria less stable (for more details see CR auctions paper).

For example, say there are three validators, a transaction with a tip of $5 and a bribing agent who values censoring the transaction at $10. If there is a single leader, it is in the leader's best interest to take the bribe for > $5 in exchange for censoring the transaction. When more leaders are added, the bribing agent must bribe each of the leaders, eventually it becomes too expensive to bribe everyone and the transaction gets through. See Censorship Resistance in On-chain Auctions for more details.

Censorship Resistance in On-chain AuctionsNotes

Notes

Duality Labs is building an on-chain MEV auction that redistribute's the value back to liquidity providers. The v1 is largely inspired by ABCI++ and being built with Tendermint and ABCI 1.0 (PrepareProposal and ProcessProposal). We plan on open sourcing a repo in Q2 2023. In the meantime feel free to reach out for partnerships and collaboration on twitter: @PossibltyResult.

Duality Labs

Big shoutout to Zaki Manian for leading us down the right path for a practical implementation of multiple concurrent block proposers.